특집

유비쿼터스 센서 네트워크의 정보보호 이슈와 동향

한국정보보호진흥원 전자거래보호단 박 종 욱, 주 학 수, 이 재 일
고려대학교 정보보호대학원 이 동 훈

차 례

Ⅰ. 서 론

최근 저전력의 무선통신과 적응형 자가조직(Self-organization)능력을 가진 초소형 마이크로 센서의 하드웨어 기술 발전으로 다양한 기능의 센서를 이용한 무선 센서 네트워크의 구축이 가능하게 되었다. 무선 센서 네트워크는 현실세계의 여러 이벤트를 감지하는 센싱 작업을 기반으로 주로 과학용이나 군사용으로 많이 사용되고 있다. 즉, 직접 접근이 용이하지 않은 전장에서의 적군감시, 열악한 환경을 모니터링 하는 지진감지, 교통의 감시와 제어를 위한 지능형 교통통제, 장기간의 관찰이 요구되는 생태감시 등 그 응용범위가 다양하게 확장되고 있다.

하지만 센서 네트워크는 기존의 네트워크와 달리 노드의 한정된 에너지원, 계산 능력의 저하 등 센서 노드의 자체 한계와 무선 ad-hoc 특성 등 네트워크에서 비롯되는 제약조건으로 인해 전달되는 데이터가 민감한 내용일 경우, 전송되는 데이터가 쉽게 노출되거나 변조될 수 있는 위협이 항상 존재한다. 본 논문에서는 센서 네트워크에서 전송되는 데이터에 대한 기밀성, 인증, 무결성, 적시성, 확장성 등을 보장하기 위한 최근의 정보보호 이슈와 연구동향을 간략히 살펴보고자 한다.

본 논문의 구성은 2장에서 무선 센서 네트워크의 관점에서 정보보호 서비스의 요구사항에 대해 살펴보고 3장에서는 무선 센서 네트워크의 제약사항을 센서 노드 하드웨어와 네트워킹 관점에서 고찰한다. 4장에서는 최근 무선 센서 네트워크 보안과 관련하여 진행 중인 연구결과를 키 관리, 기밀성, 프라이버시, 서비스거부공격, 라우팅,

노드절취의 세부 분야별로 소개하며 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 보안 요구서비스

1. 기밀성(Confidentiality)

기밀성은 통신 당사자간에 공유되는 정보가 공격자로부터 도청공격(Eavesdropping), 트래픽 분석(Traffic analysis)방법 등을 통해 노출되는 것이 방지되어야 함을 의미한다. 센서 네트워크에서 공격되는 정보의 대상은 센서 노드 식별자, 암호키 등이 될 수 있다. 일반적으로 기밀성은 DES나 RSA와 같은 암호알고리즘의 적용을 통해 제공되는데 암호알고리즘은 크게 대칭키 알고리즘과 공개키(비대칭키) 알고리즘으로 구분된다. 대칭키 암호 알고리즘은 빠르고 효율적이나 통신자간에 하나의 동일한 키를 가지므로 이를 사전에 안전하게 나눠 갖기 위한 키 분배의 문제가 항상 존재하게 된다. 반면 공개키 암호알고리즘은 키 분배의 문제는 없지만 계산량이 복잡하여 대칭키 암호 알고리즘에 비해 속도가 느린 특성이 있다. 수백, 수천 개의 노드로 구성되는 센서 네트워크의 암호키는 전체 네트워크의 데이터 기밀성을 위해 센서 노드 하나에 대한 암호키 공격의 영향이 전체 네트워크로 확산되지 않도록 세밀한 키 제어(Fine key granularity)의 특성을 가져야 한다.

2. 인증(Authentication) / 무결성 (Integrity)

인증과 무결성은 통신 수신자가 통신하고 있는 상대편 송신자가 정당한 송신자인지와 주고받는 데이터의 내용이 공격자의 불법적인 위·변조 과정 없이 원래의 메시지임을 확인할 수 있는 방법을 제공한다. 인증의 방법에는 통신 피어(Peer) 사이의 대칭키 기반의 MAC 방식과 RSA, ECDSA와 같은 전자서명 기술이 있다. 하지만 공개키 암호방식의 전자서명 기법은 계산량이 많아 아직까지 무선 센서 네트워크에 적용되기 어려운 실정이다. 반면 공격자는 세션 가로채기(Hijacking), 재생(Replay) 공격, 중간자 공격(Man In the Middle Attack)을 통해 상대 통신자로 하여금 올바른 상대방과 통신하고 있게끔 믿게 만들 수 있으므로 이에 대한 대응책이 필요하다.

3. 적시성(Freshness)

적시성은 메시지가 현재 세션의 최신 내용이며 순서가 있어 이전에 전송되었던 메시지와 중복되지 않음을 메시지 순서(Ordering) 기능과 추측되는 지연시간의 표시를 통해 제공된다. 암호학적 방법으로 시퀀스 넘버(Sequence number), 타임스탬프(Timestamp), 비표(nonce)등이 있다.

수백, 수천 개의 노드로 구성되는 센서 네트워크는 클러스터 단위로 멤버 구성이 가변적으로 이루어지므로 공유되는 암호키에 대한 적시성이 중요하다. 즉 완전 순방향 안전성(PFS : Perfect Forward Secrecy)을 제공하기 위해 이전에 사용되었던 세션키들이 재사용되지 말아야 하며 각 세션키들은 항상 최신의 정보이어야 한다. 참고로 RSA 키 전송은 약한 적시성의 형태이며 Diffie-Hellman 키 동의는 강한 적시성을 보장한다. 암호키의 적시성은 다음과 같은 이유로 보장되어야 한다.

• 키 길이 : 특정 길이(예를 들어 64-bit DES 키)의 암호키는 센서 네트워크의 보안 정책에 의해 제한될 수 있으며 같은 이유로 암호키의 사용 횟수 또한 제한될 수 있다. 이러한 것은 하나의 키가 노출되었을 경우에 공격자로 하여금 획득할 수 있는 정보를 제한하기 위함이다.

• 키 노출에 대한 위협 : 센서에 탑재되는 암호키는 공장에서 제작되는 단계나 실제 배치 후 운영 중에 노출될 수 있다. 이런 경우 완전 순방향 안전성 보장과 알려진 키 공격(Known-key attack) 방지를 통해 그 영향을 최소화해야 한다. PFS는 이전의 공유된 암호키가 노출되어도 그 후의 키 분배 과정에서 얻는 세션키의 안전성에는 영향이 없는 성질을 뜻하며 알려진 키 공격은 이전에 노출된 세션키로 앞으로의 세션키를 찾아내는 것을 뜻한다.

• 그룹 멤버 변경 : 센서 노드는 배터리 용량 고갈 등으로 인해 더 이상 작동하지 않을 수 있다. 동작불능으로 인해 그룹에서 격리되는 센서는 공격자의 절취를 통해 그룹에서 사용되는 암호키가 노출될 가능성을 제공한다. 따라서 센서 네트워크는 그룹 멤버의 변경이 있을 경우 이전 세션키를 더 이상 사용하지 말고 새로운 세션키로 즉시 갱신해야 한다.

4. 확장성(Scalability)

일반적으로 센서 네트워크는 수백, 수천 개의 센서 노드와 수십 개 미만의 Base Station(BS, Sink)으로 구성되어진다. 따라서 리소스의 제한이나 전송지연 등으로 확장성이 떨어지는 키 관리 스킴을 적용하기가 어렵다. 즉 그룹구성원이 커질수록 암호화 횟수, 키 길이 등에 따라 리소스의 사용이 증가하지 않아 적시성을 보장하고 전송지연이 발생하지 않는 효율적인 키 관리 방안이 필요하다. 따라서 네트워크 사용량이 적은 그룹이나 단순히 메시지를 포워딩하지 않고 변경하는 멤버가 많은 그룹의 경우에는 하나의 암호키보다는 그룹별로 서로 다른 암호키를 가지는 키 관리 방법을 고려할 수 있다. 이 때 그룹간 메시지의 암호화는 해당 그룹에 속하는 암호키로 재암호화하는데 이는 데이터 전송 비용이 암호화 계산비용보다 클 경우 유용하다. 즉 K1그룹에 속하는 A노드가 K2그룹의 B노드에게 상당히 긴 메시지 C를 암호화해서 보내고자 하는 경우 $E_{k1}(C) \| E_{k2}(k1)$의 형태로 키를 인캡슐레이션하여 보냄으로서 긴 메시지를 재암호화하는데 드는 비용을 절감할 수 있다.

5. 가용성(Availability)

센서 네트워크는 에너지 소비를 최소화해야 하며 네트워크의 생존성을 늘리기 위해 불필요한 키 관리 동작을 지양해야 한다. 즉, 네트워크 레벨의 중앙 집중적인 키 관리는 자칫 센서 노드하나에 대한 취약성 공격이 전체 네트워크의 위협으로 쉽게 확산 될 수 있어 선호하기 어렵다. 키 관리 측면에서 가용성 보장을 위해서는 다음과 사항들이 고려되어야 한다.

• 센서 네트워크는 불필요한 에너지 소비를 초래하는 동작을 최소화하여 센서 노드와 같은 리소스를 보호해야 한다.

• 정보보호서비스는 센싱 정보의 이용을 제한하거나 센서 네트워크가 동작하는데 제약사항을 발생시키지 말아야 한다.

• 정보보호 서비스는 단일 장애 포인트(Single Point of Failure)를 발생시키지 말아야 한다.

• 정보보호 서비스는 데이터를 전송하거나 데이터 보호서비스(센서 노드간 키 전송 또는 키 공유)를 수행할 때 발생하는 지연을 최소화해야 한다.

6. 자가 조직(Self-Organization)

센서 네트워크는 동적으로 자신의 라우팅 토폴로지나 키 관리 서비스를 재구성할 수 있어야 한다. 센서 네트워크의 특성상 구축 이전에는 네트워크의 영향범위, 인접 네트워크 수나 거리 정보, 특정 센서노드의 위치 등을 알 수 없다. 또한 메시지를 전송하는데 발생하는 정확한 오류율, 배터리 소모량을 알 수가 없다. 마찬가지로 BS

에 대한 물리적인 위치나 홉(Hop) 수 또한 사전에 정의하기 힘들다. 따라서 이러한 가변적인 상황에 적합한 안전한 라우팅 프로토콜과 키 관리 방안 등의 정보보호 서비스가 필요하다. 또한 센서 네트워크의 자가 조직형 성질은 네트워크 구축 중이나 운영되는 동안 연결이 안 되는 센서 노드들을 다룰 수 있어야 한다. 즉 배터리 고갈이나 자연재해, 재밍(jamming), 절취 등 공격자의 의도적인 행위로 센서 노드가 격리되는 경우 라우팅, 키 관리서비스 등에는 문제가 없어야 한다.

Ⅲ. 센서 네트워크 제약사항

1. 센서 노드 제약사항

1.1 배터리 파워 소모

배터리 파워는 센서 노드의 능력에 가장 큰 영향을 끼치는 요소이다. 일반적으로 센서 노드가 센서 네트워크 내에서 초기 구축되면 배터리 교환이 불가하고 다시 충전시킬 수 없다. 따라서 센서 노드의 하드웨어 구조나 정보보호 기능을 제공하는 모듈은 센서 노드의 배터리 파워의 최소 소비를 우선순위로 고려해야 한다. 센서 노드에서 배터리 자원을 소모시키는 경우는 1) 암호학적 연산량 에너지 소모와 2) 통신 에너지 소모가 있다. 1)은 주로 프로세서의 전력소비, 프로세서 클럭 주파수(Clock Frequency), 암호학적 계산에 필요한 클럭 수에 의해 결정되어 진다. 암호학적 처리시 클럭 주파수가 감소된다고 하더라도 배터리 파워는 현격히 줄어들지는 않는다. 그 이유는 대응되는 볼트(Volt)의 감소가 필요하기 때문이다. 한편 공개키 암호는 하나의 단위동작을 위해 수천, 수백만 번의 지수 연산을 필요로 하여 배터리 소모가 상당하므로 배터리 소비량은 클럭 수에 비례한다. 또한 배터리 파워는 센서 노드 자체의 계산량 뿐만 아니라 센서 노드간 암호키, 인증서, 비표, 초기 벡터(IV), 패딩값, 서명 등 보안 관련정보 전송 시 감소하게 된다. 통신 에너지 소모는 암호알고리즘, 참여 노드수, 메시지의 교환횟수, 패킷 사이즈 등에 의해 영향을 받는데 일례로 대칭키 알고리즘이나 타원곡선 암호는 RSA에 비해 교환되어야 할 파라미터가 적으므로 통신 에너지가 덜 소모된다. [표 1]은 현재 나와 있는 주요 센서노드의 하드웨어 사양을 나타내는 것으로 UC Berkeley의 MICA2DOT는 배터리의 교환 없이 1년 이상 동작된다.

1.2 전송 거리

센서 노드의 전송 거리는 배터리 파워를 보존하기 위해 제한될 수 있다. Sensoria와 Rockwell의 센서 노드는 전송 출력이 10㎽에서 100㎽로 다양하다[1]. 전송 파워를 제한하는 것은 센서 노드의 에너지를 보존하고 브로드캐스트 되는 메시지에 대한 내용이 공격자에게 노출되는 있는 위협을 해소할 수도 있다. 현재 나와 있는 센서노드는 대부분 수십~수백미터 이내의 전송범위를 갖는다. [표 1]의 버클리대 MICA2 Mote는 약 125미터의 전송거리를 갖고 UCLA의 iBadge는 10-30미터 이내의 전송능력을 갖고 있다. 그러나 BS는 1Km가 넘는 롱홀(Long-haul) 통신 능력을 갖고 ad-hoc 네트워킹을 지원하기 위해 센서 노드간 데이터 중계 역할을 수행한다.

1.3 메모리

센서 프로세서는 다양한 프로세싱을 하기 위한 서로 다른 형태의 메모리를 필요로 한다. 일반적으로 ROM, EPROM은 범용목적의 프로그램(임베디드 함수, 암호함수, 기본 네트웍 함수)을 위해 필요하고 RAM은 애플리케이션 프로그램, 센싱 정보, 중간단계의 연산결과를 저장하는데 필요하다. 또 다른 메모리 형태인 EEPROM 또는 FLASH는 다운로드된 애플리케이션 코드, 휴지(Sleep)모드간 임시데이터를 저장하는데 사용된다.

1.3.1 ROM과 RAM

현재 높은 수준의 안전성을 제공하는 암호알고리즘이라도 수십 KB 정도면 구현할 수 있어 수백KB에서 몇MB에 이르는 RAM, EPROM등 비휘발성 메모리의 크기를 제공하는 대부분의 센서에서는 암호알고리즘을 저장하는데 별다른 영향을 주지 않는다. 마찬가지로 암호 알고리즘이 수행되는데 필요한 RAM 사이즈 또한 문제가 되지 않는다. 현재 대부분의 대칭키 암호와 해쉬함수는 1KB이하의 RAM 용량 안에서 동작되고

〔표 1〕 주요 센서 노드의 하드웨어 플랫폼 사양

	UC Berkeley MOTE			Sensoria		UCLA
	MICA	MICA2	MICA2DOT	WINS 3.0	sGate	iBadge
프로세서	Atmel ATMega103 L 4㎒	Atmel ATMega128L 4㎒		Intel PXA255 (100-400㎒)	Hitachi SH-4 300 MIPS	Atmel ATMega128L 4㎒
FLASH	128KB			〈32MB + 1GB CF	16MB	128KB
SRAM	4KB	512KB		〈64MB	64MB	4KB
EEPROM	4KB			-	-	4KB
프로세서 소비전류	5.5㎃ (활성) 〈20㎂ (휴지)	8㎃ (활성) 〈15㎂ (휴지)		-	-	8㎃ (활성) 〈15㎂ (휴지)
주파수	433/916㎒	433/868/916㎒		2.4㎓	2.401-2.495㎓	2.400-2.483㎓
채널수		〉8, 〉100		〈 16	4	79
전송 소비전력	0.75㎽	-		-	10-100㎽	1㎽
전송거리	100ft	500/1000ft		-	500m	10-30m
전원	2 × AA 〈1년	2 × AA 〈1년	3V Coin Cell 〉1년	-	-	Li-Ion 3.5h - 5.4h
외부 전원	3V	2.7 - 3.3V		15V	12-15V	3.6V
LED	3 LEDs		1 LED	2 LEDs	8 LEDs	1 LED
크기	-	58×32×7㎜	25×6㎜	3½×5½in	8.4×6.0×2.7in	47×68×7㎜
무게	-	18g	3g	-	2lbs 14oz	65g
확장 커넥터	51핀		18핀	-	-	○
GPS	×			12채널 WAAS	NMEA v2.2	×
802.11	×			802.11b	802.11b/ 블루투스	블루투스
이더넷	×			10Mbit	10/100Mbit	×
RS-232시리얼	×			○	○	○
USB	×			3 포트	×	×
PCMCIA카드	×			1 슬롯	2 TypeⅡ슬롯	×
CF 메모리카드	×			2 슬롯	×	×
오디오 입출력	×			1 Stereo	×	Microphone, 스피커

비대칭키 함수는 수KB정도의 RAM을 필요로 한다. [표 1]에서 볼 수 있듯이 대부분의 주요 센서 프로세서들이 수백KB에서 수십MB에 이르는 용량을 가지고 있으므로 문제가 없으며 앞으로도 저비용, 고용량의 하드웨어 기술로 메모리 용량 문제는 없으리라 판단된다.

1.3.2 EEPROM/FLASH

센서 네트워크에서 키 관리 서비스는 동적으로 대칭키, 공개키, 개인키 등을 저장할 수 있도록 메모리 내의 내용을 수정할 수 있는 EEPROM, FLASH와 같은 고가의 프로그래머블 메모리가 필요하다. 주문형 집적회로(ASIC)에 하나의 칩으로 프로세서, RAM과 PROM을 탑재하여 상기 요구사항을 만족할 수 있으나 센서 노드가 언제나 메모리 내용을 수정할 수 있는 EEPROM이나 FLASH 메모리가 선호되고 있다. [표 1]의 Sensorial 센서는 FLASH의 메모리가 최소 16MB이상으로 RAM과 마찬가지로 암호서비스를 제공하는데 프로그래머블 메모리의 용량은 큰 문제가 되지 않는 것으로 파악된다.

1.4 위치 측정

센서 네트워크 내에서 위치인식은 각 센서 노드의 절대적 또는 상대적 위치를 GPS, 초음파, RF를 이용하여 알아낸다. [표 1]의 Sensoria WINS NG3, sGate는 GPS 기능을 탑재하고 있지만 모든 센서들이 GPS 기능을 갖는 것은 아니다. GPS를 이용하는 경우 군사용의 PPS(Precision Positioning Service)는 50m 이내, 민간용의 SPS(Standard Positioning Service)는 200m이내의 오차범위를 갖는다. 이러한 오차는 특정 위치의 좌표 값과 그 곳의 측정값과의 차이를 이용하여 보정하는 DGPS (Differential GPS)를 통해 5m이내로 줄일 수 있다. 일반적으로 센서 노드의 위치를 측정할 때는 측정신호의 도착시간 차이, 거리에 따른 신호의 감쇄정도, 상대노드에 대한 각도, 비컨(Beacon)에 근접한 정도의 정보를 이용하여 측정할 수 있다[2,3]. 센서 네트워크에서 두 개의 센서 노드가 동일한 위치에 놓일 확률은 거의 0에 가까우므로 센서 노드의 정확한 위치정보는 인증이나 라우팅에 유용하게 사용될 수 있다. 즉, 어느 지역의 센서 노드들이 공격자에게 노출되었다면 위치정보를 이용하여 해당 노드들의 키를 모두 제로화(Zeroize)하거나 갱신할 수 있다.

1.5 물리적 보안모듈(Tamper Resistance Module)

센서 노드의 저비용 정책으로 대부분의 센서 노드들은 탬퍼링 방지기능이 없어 메모리의 내용을 노출시키는 물리적 공격에 약하다. 물리적 보안모듈은 능동형(Active)과 수동형(Passive)의 두 가지의 형태로 나눌 수 있다. 능동형은 하드웨어 회로 형태로 별도의 에너지를 소모하나 민감한 데이터를 보호할 수 있다. 그러나 수동형은 보호코팅(Protective Coating)처럼 내부 회로의 변조 여부를 탐지할 수 있는 기능만을 제공한다. 센서 네트워크에서 몇 개의 센서노드가 공격자의 손에 넘어갈 수 있는 개연성이 충분히 있고 한번 배치되면 유지관리가 어려우므로 수동형의 물리적 보안모듈은 제조 단계 후 배치이전의 기간동안 변조가 없었는지 제한적인 상황에서만 이용될 수 있다. 참고로 현재 가능한 물리적 공격으로는 스마트카드에 적용되는 프로브 공격이나 TEMPEST 공격이 RFID기반의 센서 노드에도 그대로 적용될 수 있다[4]. 또한 센서 노드의 설계자가 예기치 못한 정보를 이용하는 전력해석(Power Analysis), 타이밍 해석(Timing Analysis) 등의 부채널 (Side Channel) 공격도 가능하다.

1.6 시각

Time-critical한 정보를 다루는 센서 노드에서 시각은 전체 네트워크의 동기화를 위해 필요하다. 반면 공격자는 센서 노드가 시각에 따른 민

감한 정보를 BS로 송신할 때 타임스탬프 정보를 변경할 수 있다. 따라서 시각 정보는 스푸핑(Spoofing)의 위협으로부터 안전해야 하는데 GPS는 안전한 시각 정보원의 한 예이다. GPS를 이용할 수 없는 센서 노드는 로컬환경의 정확한 시각정보나 TCP/IP기반의 NTP(Network Time Protocol)의 사용을 고려할 수 있을 것이다.

2. 네트워킹 제약사항

2.1 Ad-hoc 네트워킹

센서 네트워크는 ad-hoc 특성으로 네트워크 토폴로지나 라우팅 구조가 수시로 변경된다. 이러한 성질은 센서 노드가 네트워크의 생존성을 위해 여러 가지 역할을 수행하기 위한 복합적인 사전설정이 필요함에도 불구하고 사전에 의도하는 대로 충분히 할 수 없는 상황을 초래하게 한다. 또한 센서 네트워크는 시간, 날씨, 전장 등 환경의 조건에 따라 발생하는 채널 페이딩(Fading), 가용 전력과 이벤트 발생에 의한 노드의 슬립(Sleep) 모드에 따라 네트워크의 연결이 지속적으로 이루어지는 것이 아니라 간헐적으로 이루어지게 된다. 이렇게 센서의 가용성에 제약을 주는 ad-hoc 네트워킹은 정보보호측면에서 암호화키를 포함하는 메시지나 디지털 크리덴셜 정보를 포함하는 메시지의 전달을 항시 신뢰할 수 없게 만든다. 따라서 암호학적 동기화 이슈가 발생하고 때때로 패킷의 손실로 특정 노드의 고립을 유발시킬 수 있다.

2.2 데이터 전송속도/패킷 사이즈

데이터 전송속도와 패킷 사이즈는 센서 노드의 에너지 소비량과 비례한다. 센서 네트워크의 패킷 사이즈는 일반적인 패킷 통신과 비교했을 때보다 작으며 데이터 처리속도 또한 수~수십Kb 이하로 낮다. 따라서 에너지 소비량과 메시지 오버헤드의 부담을 경감하기 위해 적절하게 짧은 패킷사이즈를 고려해야 한다. 키 관리 등 정보보호 서비스의 경우에도 정해진 패킷사이즈 범위 내에서 적용할 수 있는 프로토콜의 개발이 필요하다. 반면 낮은 데이터 처리속도는 네트워크 지연을 발생시킬 수 있어 암호키 공유시 동기화 문제가 발생할 수 있으므로 이에 대한 해결방안이 필요하다.

2.3 채널 에러 / 지연

데이터 링크 계층처럼 하위 계층의 통신 프로토콜은 에러 탐지나 에러교정 서비스를 제공하나 기밀성, 무결성, 인증 등의 서비스가 적용되는 상위 계층에 에러가 파급되면 애플리케이션 데이터의 검증과정에 영향을 주게 된다. 예를 들어 DES 암호알고리즘은 피드백 또는 체이닝(Chaining) 운영모드에 따라 전체 메시지에 대한 에러 파급범위가 다르므로 센서 네트워크 특성에 맞는 암호알고리즘의 운영모드가 필요하다.

반면 멀티 홉 라우팅은 패킷이 네트워크를 통해 전달되면서 지연을 발생시킬 수 있다. 혼잡도(Congestion)와 노드에서의 프로세싱 처리속도는 지연의 정도를 결정한다. 따라서 커브로스(Kerberose)와 같이 유효기간을 포함한 토큰을 사용하는 인증프로토콜이 사용될 경우 동기화 에러가 발생하지 않도록 네트워크 지연을 최소화 시켜야 한다.

2.4 일방향 통신

모든 센서 노드가 쌍방향 통신능력을 가진다고 가정하기는 어렵다. 하드웨어 특성과 노드의 역할에 따라 센서 노드는 데이터를 송신만 하거나 반대로 수신만 할 수도 있을 것이다. 예를 들어 적지의 탱크 움직임을 관찰하는 전장의 센서 노드는 자신의 존재 자체가 적에게 노출되는 것을 방지하기 위해 데이터를 수집하고 분석할 뿐이지 적에게 탐지될 위험이 사라지기 전까지는 아군에게 데이터 전송은 하지 않을 수 있다. 따라서 이러한 일방향 통신 특성은 암호키 분배 프로토콜의 유형을 제한할 수 있게 된다.

2.5 잦은 라우팅 변경

센서 네트워크에서는 BS의 배터리전력이 소진되어 BS의 기능을 다른 센서 노드로 이양시킬 수 있다. 동시에 ad-hoc 특성으로 인한 그룹구성원의 잦은 변경으로 라우팅 과정에서 중간단계의 노드가 바뀔 수 있다. 따라서 이 때 안전하게 라우팅 토폴로지를 변경시킬 수 있어야 한다. 라우팅 프로토콜은 센서 네트워크의 노드 밀집도에 따라서 라우팅 성능이 결정될 수 있는데 강한 연결성을 갖는 라우팅 토폴로지를 위해 노드 수는 1000개, 클러스터 사이즈는 10개 정도를 전형적인 센서 네트워크로 보고 있다[5]. 추가적으로 보안서비스가 단대단 방식이 아니라 홉단위(hop-by-hop)로 이루어질 경우 잦은 라우팅 정보의 변경은 동시에 보안서비스에 많은 오버로드를 초래하게 된다. 예를 들어 Pairwise 방식의 키 관리서비스는 이웃 노드가 변경됨으로써 새로운 이웃 노드와의 암호키 분배가 다시 수행될 필요가 있다.

Ⅳ. 최근 정보보호 이슈와 동향

1. 키 관리

센서 네트워크의 정보보호 서비스를 구축할 때 우선적으로 해야 할 사항 중에 하나는 센서 네트워크 운영 시 사용될 암호키를 설정하는 것이다. 지난 수십 년 동안 다양하고 효율적인 키 관리 프로토콜이 연구되어 왔지만 동일한 프로토콜을 센서 네트워크에 적용하는 것은 한계가 있다. 즉 대부분의 센서 장비들은 컴퓨팅 파워의 제약이 있어 공개키 암호방식의 키 관리 프로토콜을 적용하는 것이 어렵다. 더구나 수백, 수천 개의 노드로 구성되는 센서 네트워크에서의 키 관리 프로토콜은 확장성이 있어야 한다. 지금까지 연구결과 중 가장 간단한 솔루션은 네트워크 레벨의 단일 암호키를 사용하는 것이다. 그러나 하나의 노드로부터의 암호키 노출은 네트워크 전체 트래픽의 내용을 노출시키는 단일 장애 포인트를 초래할 수 있다. 변형된 방법으로 하나의 암호키를 이용하여 링크계층의 단대단 암호화 세션키를 설정하는 데 사용하고 세션키가 설정된 후 암호키를 삭제하는 것이다. 그러나 이 방법 또한 초기 구축 후 그룹 멤버의 변경이 있을 경우 새로운 멤버를 추가하는 것은 불가능하다. 각각의 센서 노드간에 유일한 암호대칭키를 미리 설정하는 방법이 있으나 n개의 센서 노드가 있을 경우 각각의 노드는 n-1키를 저장해야 하고 전체적으로는 n×(n-1)/2개의 키가 필요하므로 확장성이 떨어진다.

믿을만한 BS로부터 키를 부트스트랩핑(bootstrapping) 하는 방법도 있다[6]. 각각의 노드는 BS와 오직 하나의 키만을 공유하고 다른 노드와의 암호화 통신은 BS를 통해 하는 것이다. 이러한 방법은 BS가 집중 공격을 당할 위험이 있으므로 물리적 공격에 대비해 BS내에 물리적 보안모듈이 보강되어야 한다.

최근 랜덤-키 사전분배(Random-key Predistribution) 프로토콜에서는 매우 큰 대칭키 풀을 선택하고 여기서 무작위로 키를 선택하여 각 센서 노드에게 할당하는 방법을 제안하였다[7]. 통신하고자 하는 두 개의 노드는 자신의 대칭키 풀을 탐색하여 상대방과 같은 공통키를 소유하고 있는지 판단하여 만일 동일한 공통키를 소유한다면 세션키를 설정하게 된다. 이러한 방법은 신뢰할 수 있는 BS가 없어도 됨을 의미하는 것이다. 그러나 공격자가 많은 노드에 대해 공격을 성공시키는 경우 공격자는 완전한 대칭키 풀을 구성할 수 있는 취약성이 존재한다.

키 관리 프로토콜 관련해서 앞으로는 개선된 랜덤-키 사전분배 프로토콜이 연구되어야 한다.

또한 타원곡선 공개키 암호방식과 같은 공개키 암호방식을 적용할 수 있는 하드웨어 개발이 병행되어야 할 것으로 판단된다.

2. 비밀성과 인증

전통적인 네트워크와 같이 센서 네트워크의 애플리케이션 또한 패킷의 도청, 추출, 변경에 대한 보호가 필요하다. 점대점(Point-to-Point) 통신을 위한 단대단(End-to-End) 암호화 기법은 고수준의 정보보호 서비스를 제공하지만 센서 노드들이 암호화 통신을 하기 위해 통신하고자 하는 센서노드별로 각각 다른 키를 저장하고 있어야 하기 때문에 비실용적이라 할 수 있다. 이에 센서 네트워크 설계자들은 단대단 암호화방식보다 각 노드가 이웃하는 노드와 공유해야 하는 하나의 암호키만을 저장하는 방식인 홉대홉(Hop by Hop) 암호화 방식을 주로 사용한다. 이 경우, 하나의 노드를 제어하고 있는 공격자가 자신의 노드를 통한 암호문을 복호화할 수 있는 문제가 있다. 이러한 문제는 공격자가 수많은 통신이 자신의 노드를 경유하도록 조작하는 경우 심각한 문제가 될 수 있다. 대안으로 하나의 메시지를 나누어 여러 개의 서로 다른 패스를 통해 전달하고 최종 목적지에서 재배열하여 원래 메시지를 얻어내는 Multipath routing protocol 등과 같은 안전한 기술들이 등장하고 있다.

인증기술은 크게 공개키 기반(PKI) 방식과 브로드캐스트 암호를 기반한 방식으로 구분할 수 있다. 공개키 암호방식에 비해 브로드캐스트 암호 방식의 장점은 크게 두 가지를 생각할 수 있다. 첫째, 브로드캐스트 암호화 방법은 대칭형 암호알고리즘을 사용하기 때문에 공개키 암호방식보다 빠르며 또한 디바이스로 하여금 낮은 오버헤드를 갖게 함으로써 디바이스 제조업자와 사용자들이 비용을 절감할 수 있다. 둘째, 프로토콜이 일방향으로 진행됨으로써, 공개키 방식의 양방향 프로토콜 방식보다 안전하다는 점이다. 보통 공개키 시스템은 링크계층에서 암호키를 공유하기 위한 핸드쉐이크 과정이 일어나는데, 이 과정에서 두 개의 취약점을 가지고 있다. 먼저 비밀키를 찾기가 쉽고, 컨텐츠가 보호되지 않는 인터페이스를 찾기가 더 쉽다. 실제 사례로 Beale Screamer가 공개키 암호 시스템을 사용하고 있는 Windows Media Player를 공격하여 성공한 바 있다. 공개키 암호방식에 비해 브로드캐스트 암호방식의 단점은 부인봉쇄 서비스를 지원해주지 못한다는 것이지만 센서 네트워크의 자원, 저장 공간 등을 고려한다면 공개키 암호기반보다는 TESLA[8] 등과 같은 브로드캐스트 암호를 기반으로 한 인증에 대한 연구가 활발해 질 것으로 판단된다.

3. 프라이버시

정보수집의 도구로 볼 수 있는 센서네트워크에서 공격자는 저장된 센서데이터에 접근하거나 네트워크에 쿼리 혹은 도청방법을 통해 사용자의 기밀정보를 얻어낼 수 있다. 특히 최근 센서네트워크의 센서로 사용될 수 있는 RFID 기술은 사람, 제품, 현금의 추적에 사용되어 개인의 프라이버스 침해위험이 매우 높다. 이러한 프라이버시 위험요인에 대해 W3C의 P3P 표준 설계자인 Marc Langheinrich는 유비쿼터스 환경에서 사용자의 프라이버시 보호를 위해 [표 2]와 같은 6가지 설계원칙을 제안하였다.

센서 네트워크에서도 프라이버시 이슈가 부각된다. 가장 분명한 리스크는 유비쿼터스 센서 기술은 악의적인 공격자가 인지하지 못하는 불특정 다수를 대상으로 비밀스러운 탐색이 가능하다는 점이다. 예를 들어 상점 주인은 고객들은 비밀리에 모니터링할 수 있고 이웃 주민들은 이웃의 행동을 관찰할 수 있다. 또한 법 집행기관은 공공의 장소의 대중의 행동을 감시할 수 있다. 센서

〔표 2〕 프라이버시 보호를 위한 설계원칙

설계원칙	정의
Notice	사용자 관련 어떤 데이터가 수집되고 있는지 항상 사용자에게 알려야 한다.
Choice and Consent	사용자는 자신의 어떤 정보가 사용될 것인지를 선택할 수 있어야 하며, 사용자의 동의하에 수집되어야 한다.
Anonymity and Pseudonymity	사용자의 프라이버시보호를 위해 사용자가 익명 및 가명정보를 이용할 수 있어야 한다.
Proximity and locality	데이터를 사용하고자 하는 사용자의 위치를 기반으로 접근을 제한할 수 있는 근접정보 및 장소 정보 등을 이용할 수 있는 메커니즘이 필요하다.
Adequate Security	다양한 상황에 따라 변하는 보호기법들이 다양해져야 한다.
Access and Resources	사용자는 자신의 데이터에 대한 접근권한을 갖고 있어야 한다.

가 점차 소형화, 미립자화되고 숨기기 쉬운 상태로 발달하면서 프라이버시 침해의 우려가 점점 높아지고 있는 게 현실이다. 또 다른 문제점은 비록 센서 네트워크가 구축 초기 당시 합법적인 목적으로 구성되었다 할지라도 후에 예상치 못한 불법적인 용도로 사용되어 질 수 있는 가능성이 있다는 점이다.

센서 네트워크 환경에서 PET(Privacy Enhancing Technology) 등과 같은 사용자의 프라이버시 보장을 위한 기술이 적용될 수 있지만 기술만으로는 프라이버시 문제를 해결할 수 없다. 그 보다는 사회규범, 새로운 법, 기술적 대응방안들의 혼합으로 해결되어야 한다. 일례로 센서 노드의 존재와 데이터 수집에 대한 대중의 인식이 매우 중요하다. 영향 받는 당사자의 신뢰 속에서 센서 네트워크 기술을 수용할 수 있어야 하는 것이다.

4. DoS 공격

공격자는 DoS 공격을 통해 무선 센서 네트워크의 가용성을 심각하게 침해할 수 있다[9]. 가장 간단한 예로 공격자는 많은 전력을 필요로 하는 시그널을 브로드캐스팅 함으로써 네트워크의 운영을 중단시킬 수 있다. 좀 더 지능적인 위협으로 공격자는 802.11 MAC 프로토콜을 공격함으로써 통신 장애를 발생시킬 수 있다. 즉 이웃 노드와 동시에 전송한다거나 Request-to-send 시그널로 채널 액세스를 지속적으로 요청할 수 있을 것이다.

재밍에 대한 대표적인 방어 메커니즘은 스펙트럼 확산 통신방식을 적용하는 것이다[10]. 아직 암호학적으로 안전한 스펙트럼 확산 라디오는 상업적으로 이용할 수 없는 상황이며 게다가 이러한 방법은 공격자가 불법적으로 노드를 절취한다거나 암호키를 획득했을 경우에는 무용지물이 된다. 그러나 센서 네트워크가 재밍 공격에 탐지능력이 있고 재밍이 네트워크의 일부분에서만 일어난다면 센서 네트워크는 재밍 지역을 파악하여 라우팅을 우회할 수 있도록 할 수 있다[11]. 이 영역의 진일보된 발전은 DoS 공격에 대한 개선된 방안을 제공하리라 기대된다.

5. 라우팅

센서 네트워크에서 라우팅과 데이터 전달은 통신을 가능하게 하는 필수서비스이나 현재의 라우팅 프로토콜은 많은 보안 취약성을 내재하고 있다[12]. 공격자는 라우팅 프로토콜에 대해 DoS 공격을 가해 통신을 단절시킬 수 있는데 간단한 일례로 거짓 라우팅 정보를 네트워크에 주입함으로서 라우팅 정보의 불일치가 일어나게 할 수 있다. 인증을 통해 거짓 정보 삽입 공격을 막을 수 있지만 아직까지 몇몇 라우팅 프로토콜은 공격자가 정당한 라우팅 메시지를 통해 이루어지는 재연공격에 취약하다[13]. 게다가 라우팅 프로토콜은 특히 노드 절취 공격에 취약하다. 예를 들어

최근의 연구결과에 따르면 모든 라우팅 프로토콜은 단 하나의 절취된 노드로부터의 공격에 대해 전체 네트워크가 영향을 받을 정도로 매우 취약한 것으로 분석되었으므로[12] 이에 대한 심도 있는 연구가 뒤따라야 할 것으로 판단된다.

6. 불법적인 센서노드 절취

센서 네트워크는 물리적 보안이 당연시 여겨졌던 이전의 컴퓨팅 환경과 달리 센서 노드들이 임의의 장소에 무인상태로 산재하기 때문에 노드의 절취, 획득 등 공격자로부터의 물리적 보안에 취약하다. 공격자는 이러한 절취를 통해 센서 노드 안에 있는 암호학적 비밀정보를 빼내고 내부 프로그래밍 모듈을 변경하여 정상적인 노드인 것처럼 가장할 수 있게 된다. 물리적 보안모듈이 높은 강도의 보안서비스를 제공하나 아직까지는 비싼 단점이 있다.

첫 번째 대안으로 때로는 소프트웨어적인 알고리즘을 적용할 수 있다. 예를 들어 센서 네트워크 전반에 상태정보를 복사하고 이를 전송하여 불일치가 일어나는 노드를 탐지하는 메커니즘을 고려할 수 있다. 노드의 불법적인 절취에 대비하기 위해 다수의 독립적인 경로에 각각 패킷을 보낸 후 최종 종착지에서 이상이 있는 패킷을 확인하는 라우팅 프로토콜이 제안된 바 있다[14].

두 번째 방법으로 환경에 대한 다수의 잉여정보(redundancy)를 수집한 다음 이것이 일치하는지 상호 검사하는 방법이 있다. 예를 들어 네트워크가 어떤 이벤트에 대한 응답을 하기 전에 여러 개의 사전정보들이 필요하다면 각 노드들로부터 데이터가 수집될 것이다. 이 때 수집된 정보의 평균치로부터 멀리 떨어진 데이터들은 비정상적인 데이터로 간주하고 무시될 수 있다. 사실 잉여정보에 바탕을 둔 방어책은 센서 네트워크에 적합하다고 볼 수 있다. 왜냐하면 저가격의 매우 많은 센서 노드들이 연결되는 구조는 고가격의 적은 수로 이루어진 디바이스들보다 네트워크 전체의 효율성이 나을 수 있기 때문이다.

V. 결 론

무선 센서 네트워크의 하드웨어 플랫폼 제약과 ad-hoc 운영 환경의 특징으로 인해 보안 서비스는 기존 네트워크에 비해 상당한 위협을 받고 있다. 그러나 이러한 위협은 센서 네트워크의 기술발전이 초기 단계이므로 개선된 정보보호 솔루션을 디자인하여 대처할 수 있는 기회가 아직 남아 있는 것으로 볼 수 있다. 또한 많은 애플리케이션이 지역적이고 독자적인 하나의 관리영역 하에서 운영되므로 배치환경의 특성, 범위, 잉여정보 등을 파악하여 초기 구축 시 해당 센서 네트워크에 특화된 서비스를 디자인 할 수도 있다. 따라서 이를 위해 앞으로 많은 연구가 수행되어야 한다. 도청, 프라이버시 침해, 노드 절취, 서비스거부공격, 라우팅 정보변경 등을 막아 안전한 네트워크를 구성해야 하며 동시에 센서 노드의 리소스 제약을 해결하여 센서 노드에서도 효율적인 공개키 암호 시스템의 구현이 가능하도록 해야 할 것이다.

참 고 문 헌

[1] Rockwell WINS, http://wins.rsc.rockwell.com

[2] J. Werb, C. Lanzl, 'Designing a Positioning Systems for Finding Things and People Indoors', IEEE Spectrum, September 1998

[3] A. Savvides, C. Han, M.B.Srivastava, 'Dynamic Fined-grained Localization in Ad-hoc Networks of Sensors', MobiCom 2001, July, 2001

[4] Sarma, S. et al, 'RFID Systems and

Security and Privacy Implications', Workshop on Cryptographic Hardware and Embedded Systems, LNCS, 2002

[5] Mills, D., 'Low Energy Communications and Routing for Microsensor Networks', Proceedings of the ARL Federated Laboratory 4th Annual Symposium, 21-23 March 2000.

[6] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J.D. Tygar, 'SPINS: Security Protocols for Sensor Networks', Wireless Networks Jorunal(WINE), September 2002

[7] Laurent Eschenauer, Virgil D. Gligor, 'A Key Management Scheme for Distributed Sensor Networks', ACM CCS'02, October 2002

[8] Donggang Liu, Peng Ning, 'Multi-Level u-TESLA: A Broadcast Authentication System Distributed Sensor Networks', 2003

[9] Wood, A., Stankovic,J., 'Denial of service in sensor networks, IEEE Computing, October 2002

[10] Adamy, D., 'EW 101: A First Course in Electronic Warfare', Artech House Publishers, Norwood, MA, 2001

[11] Wood, A., Stankovic, J., Son, S., 'JAM: A mapping service for jammed regions in sensor networks', IEEE Real-Time Systems Symposium, December 2003

[12] Karlof, C., Wagner, D., 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures', IEEE International Workshop on Sensor Network Protocols and Applications, May 2003

[13] Hu, Y. C., Perrig, A., Johnson, D., 'Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks', IEEE Infocom 2003, April 2003

[14] Deng, J., Han, R., Mishra, S. 'A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks', IPSN 2003, April 2003

박 종 욱

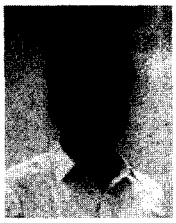
1998년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2004년 2월 : 고려대학교 정보보호대학원 공학석사
2004년 3월 ~ 현재 : 고려대학교 정보보호대학원 박사과정
1998년 3월 ~ 2000년 5월 : 삼성SDS
2000년 5월 ~ 현재 : 한국정보보호진흥원 선임연구원

<관심분야> 유비쿼터스 정보보호, 암호프로토콜

주 학 수

1997년 8월: 고려대학교 수학과 졸업
1999년 8월: 고려대학교 수학과 이학석사(대수학 전공)
2001년 8월: 고려대학교 수학과 박사과정 수료
2001년 9월 ~ 현재: 한국정보보호진흥원 연구원

<관심분야> 암호학, 공개키암호, 응용보안프로토콜



이 재 일

1986년 2월 : 서울대학교 계산통계학과 학사
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월 ~ 1996년 6월 : 한국 IBM
1996년 7월 ~ 현재 : 한국정보보호진흥원 전자거래보호단장

<관심분야> 정보보호, 유·무선PKI, 유비쿼터스 보안

이 동 훈

1984년: 고려대학교 경제학과 졸업
1987년: Oklahoma Univ. 전산학과 석사
1992년: Oklahoma Univ. 전산학과 박사
1993년 ~ 2000: 고려대학교 전산학과 교수
2000년 ~ 현재: 고려대학교 정보보호 대학원 교수

<관심분야> 암호이론, 정보보호 프로토콜, 계산이론